eurecat
Centre Tecnològic de Catalunya

Ciberseguretat a la indústria 4.0

Dr. Juan Caubet
juan.caubet@eurecat.org
Director Unitat IT Security

Innovant amb les empreses

Unitat IT Security (i OT Security)

Ciberseguretat

Criptografia

Seguretat Distribuïda

Identitat Digital i Privacitat

Cybercrime (Deep Web), **Cyber Threat Intelligence** (Prevenir, detectar i respondre a ciberamenaces sofisticades), **Ethical Hacking** (Dispositius mèdics, Dispositius IoT, PLCs, ECUs, etc.), **Radio Frequency Security** (SDR), etc.

Seguretat Distribuïda (Cloud, Fog & Edge Computing), **Seguretat en Plataformes Mòbils**, **Intel·ligència Artificial** (Machine & Deep Learning), **SDLC Segur**, **Criptografia Postcuántica**, **Tecnologia Blockchain**, etc.

Sistemes Control d'Access, **Autenticació Adaptativa**, **Autenticació Implícita**, **User-Centric Approaches**, **Identitat i Blockchain**, **Interoperabilitat**, etc.

Eurecat was Involved in writing ENISA report on recommendations in electronic identity systems authentication.

ÍNDEX

Introducció

Boletín Semanal de Ciberseguridad Industrial

¿No lo ve bien?
Ábralo en el navegador.

Centro de Ciberseguridad Industrial

Boletín Semanal

21 de noviembre de 2016
Número 182

Comentario del editor

Semana tras semana, los ciberproblemas siguen afectando a empresas de todos y cada uno de los sectores económicos. En los últimos días, y como consecuencia de sendos robos de información, han ocupado los titulares un par de nombres conocidos: Michael Page, la firma internacional de selección de personal con sede en el Reino Unido, y FriendFinder Networks, la empresa matriz de portales web como AdultFriendFinder.com, la sede web que se define a si misma como "*la comunidad de sexo más mundana y grande del Mundo*".

El risc està sempre present

Ready
Prepare. Plan. Stay Informed.
FEMA


Biological Threats


Chemical Threats


Cyber Attack


Drought


Earthquakes


Explosions

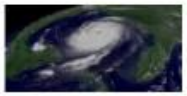

Extreme Heat


Floods


Hazardous Materials Incidents


Home Fires


Household Chemical Emergencies


Hurricanes


Landslides & Debris Flow


Nuclear Blast


Nuclear Power Plants


Pandemic


Power Outages

Radiological Dispersion Device


Severe Weather


Snowstorms & Extrer Cold


Space Weather

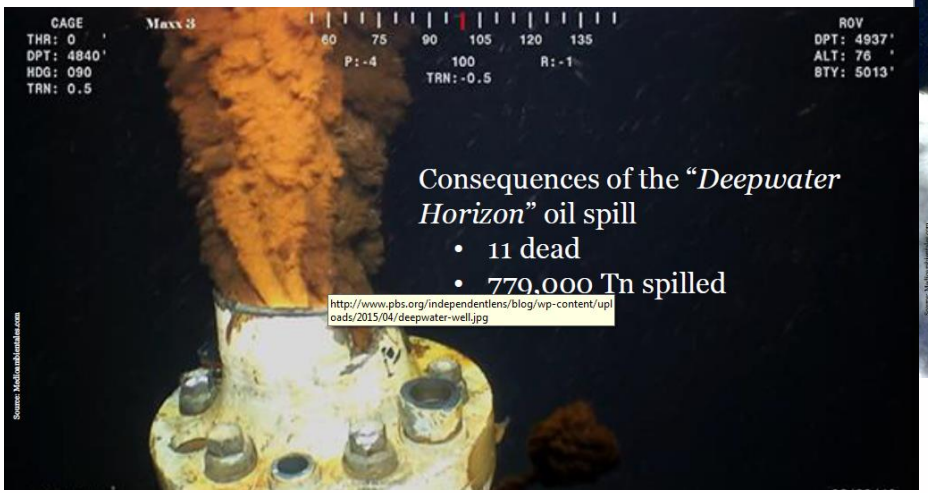

Thunderstorms & Lightning


Tornadoes


Tsunamis


Volcanoes

El risc està sempre present de manera accidental



El risc està sempre present de manera intencionada

TEKCRISPY CIENCIA TECNOLOGÍA CULTURA PLAYERONE MÁS

SEGURIDAD

Detectan nuevas vulnerabilidades en el protocolo de seguridad WiFi WPA2

Por **Rosselyn Barroyeta** - Oct 2, 2018

El año pasado, miles de usuarios quedar
de ataque que vulneró el protocolo de se

Si bien, en su momento el ataque fue cor
ha revelado una nueva falla de seguridad

REDES ZONE ANÁLISIS CURSOS ONLINE ROUTERS WIFI PLC TEST DE VELOCIDAD REDES

MANUALES FIRMWARES BITTORRENT ANDROID GNU LINUX D-LINK HOGAR DIGITAL

Chips del fabricante Infineon generan claves RSA que no son seguras

Escrito por Adrián Crespo 17 octubre, 2017 a las 9:00

seguridad 0 Comentarios

ADSLZONE.net FOROS SOPORTE OFICIAL ACTUALIDAD TUTORIALES UTILIDADES IA HUAWEI

Es noticia Ver DAZN Extranjero Internet Satélite Tarjetas Pago Virtuales Series infantiles Fibra barata Mo

700 millones de móviles Android chinos venían con una puerta trasera preinstalada

700 millones de móviles Android chinos venían ...

telefonía 6

Una de las ventajas que tiene Android es que, al ser código libre, cualquier fabricante puede compilar su propio sistema y modificarlo a su gusto (hasta cierto punto, siguiendo las guías que establece Google). El problema es que algunos fabricantes, en este caso chinos, pueden tomarse esto con demasiada libertad, y pueden aprovechar para **obtener datos de los usuarios que utilizan sus teléfonos.**

El risc està sempre present de manera intencionada

‘Denial of service’ attack disrupted US energy company operations, government confirms

Zack Whittaker @zackwhittaker / 5 hours ago

Comment

Norway's Norsk Hydro lost $50 million in cyber attack

AFP/The Local
news@thelocal.no
@thelocalnorway

30 April 2019
12:52 CEST+02:00

norsk hydro

Share this article

Norsk Hydro was targeted in a cyber attack. Photo: Bjoertvedt/Wikimedia Commons

A cyber attack that targeted Norwegian industry giant Norsk Hydro in March cost the company around $50 million.

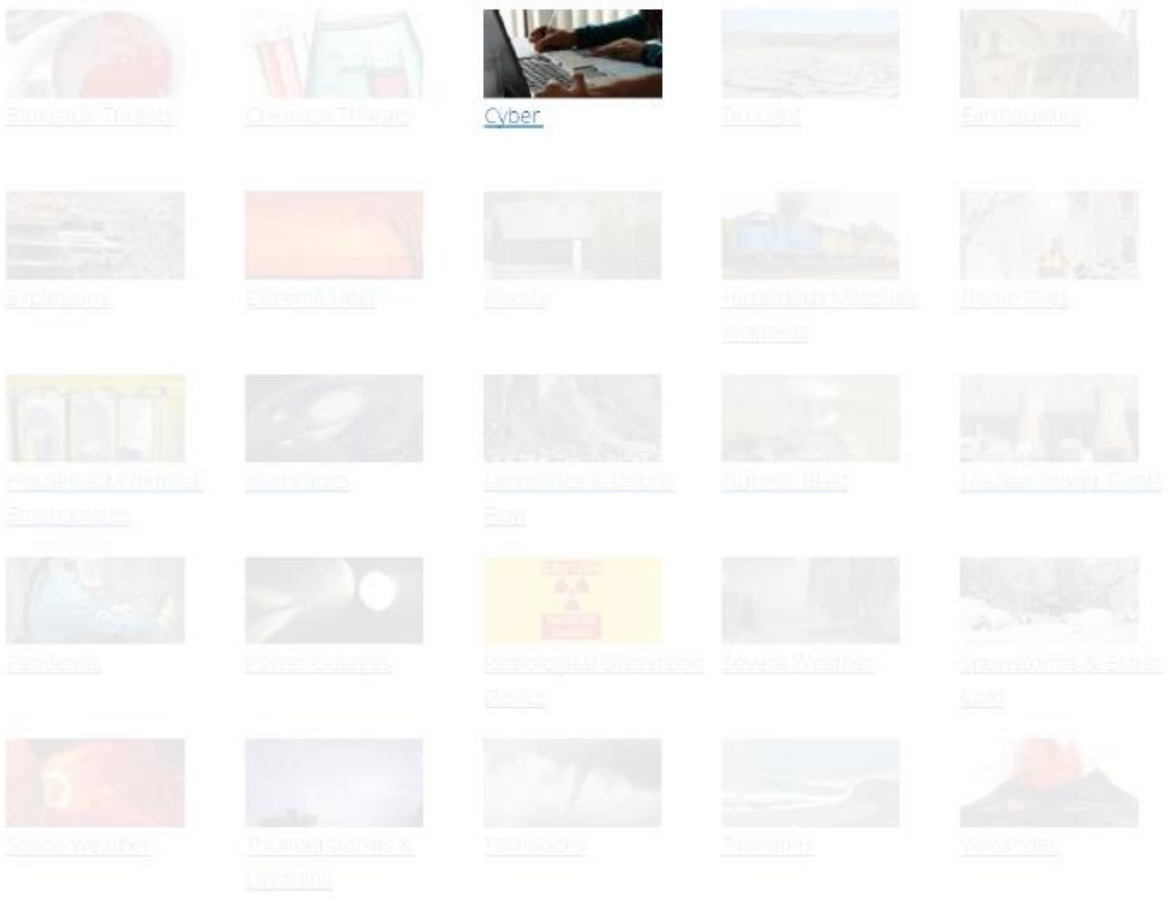
El risc està sempre present de manera intencionada

We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.

One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.
In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.
This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression.

- Cutting Sword of Justice

El risc està sempre present



El risc està sempre present... i no ho percebem

L'equació del risc

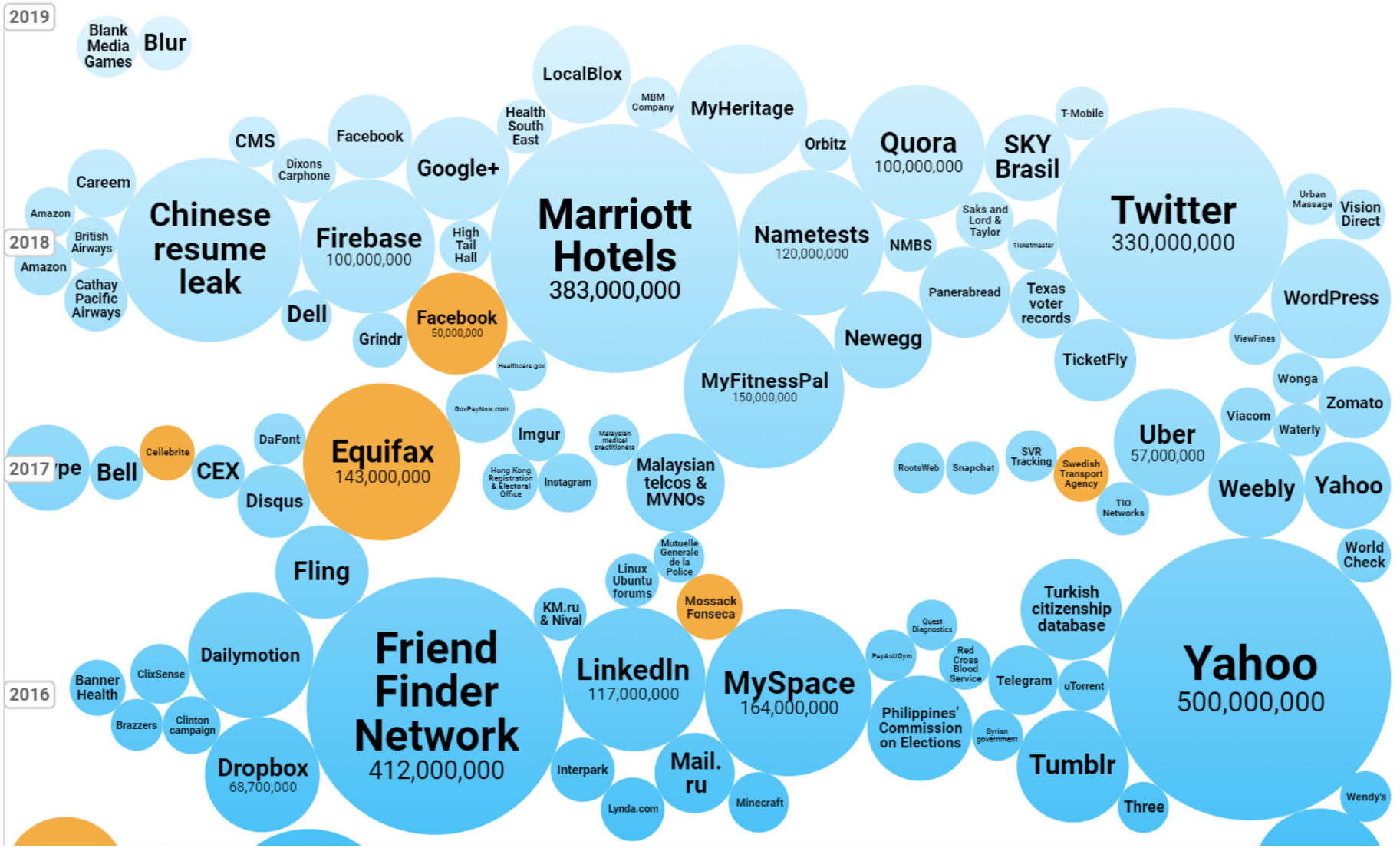
Risc = Amenaça x Vulnerabilitat x Impacte

Amenaça: Circumstancia o esdeveniment que te el potencial de causar danys.

Vulnerabilitat: Debilitat que pot ser explotada per un adversari o a través d'un incident.

Impacte: Quantitat de pèrdua o dany que es pot esperar després d'un atac exitós.

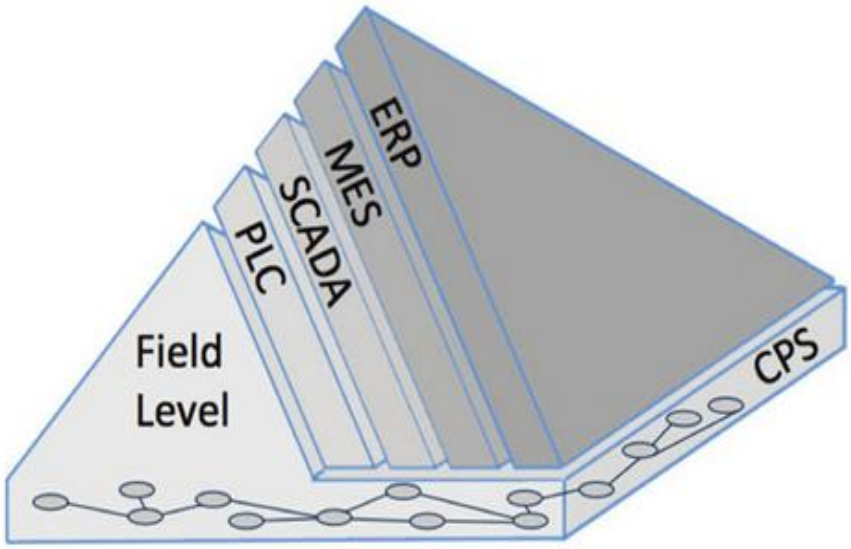
La realitat es...



Indústria 4.0

La Indústria 4.0

Piràmide d'automatització industrial clàssica.



Piràmide d'automatització industrial a Indústria 4.0.

Dispositius Intel·ligents

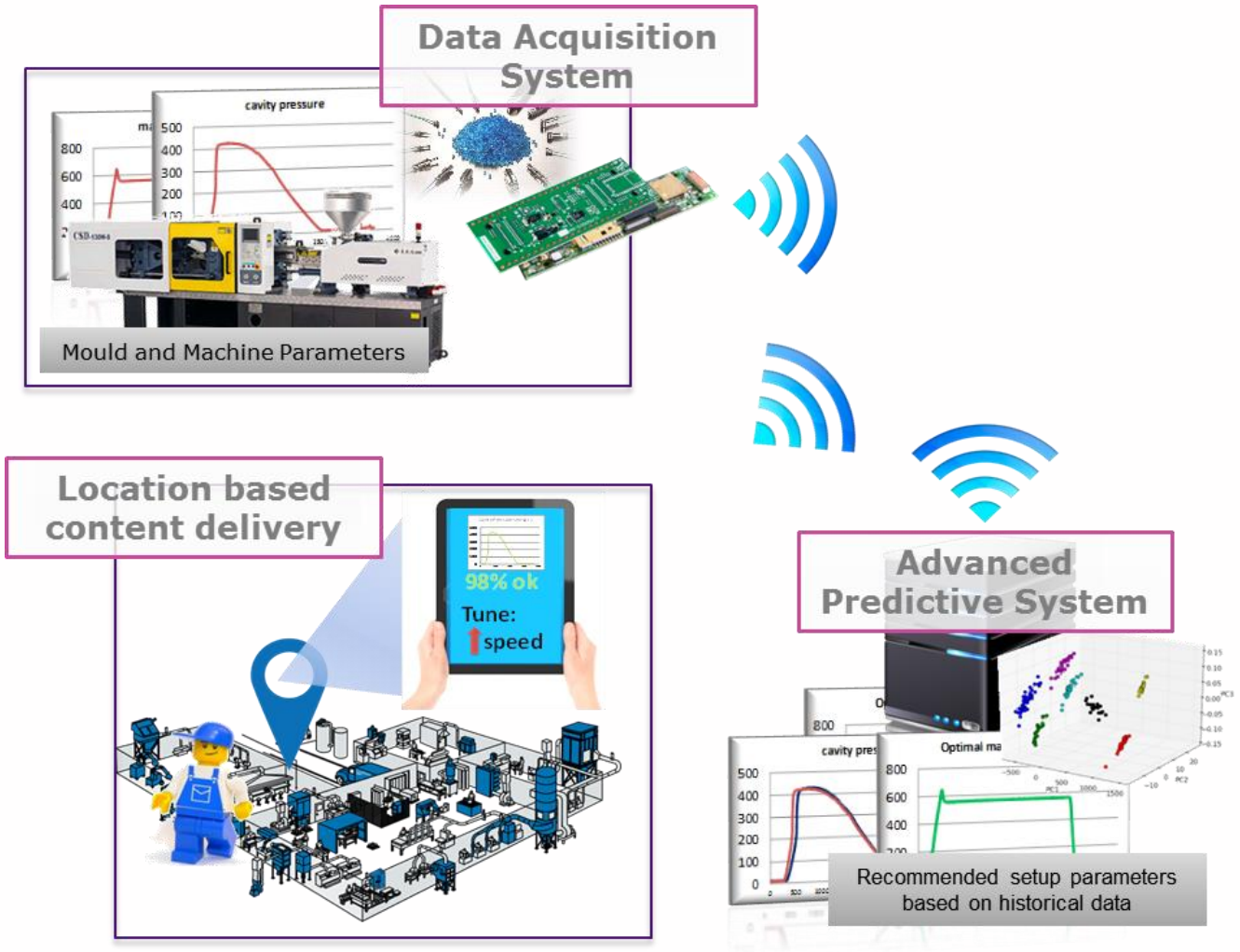
Internet of Things (IoT)

- Hot reconfiguration
- Near-real time information (encoder status)
- Adaptation to factory (interoperability and delocalized framework)

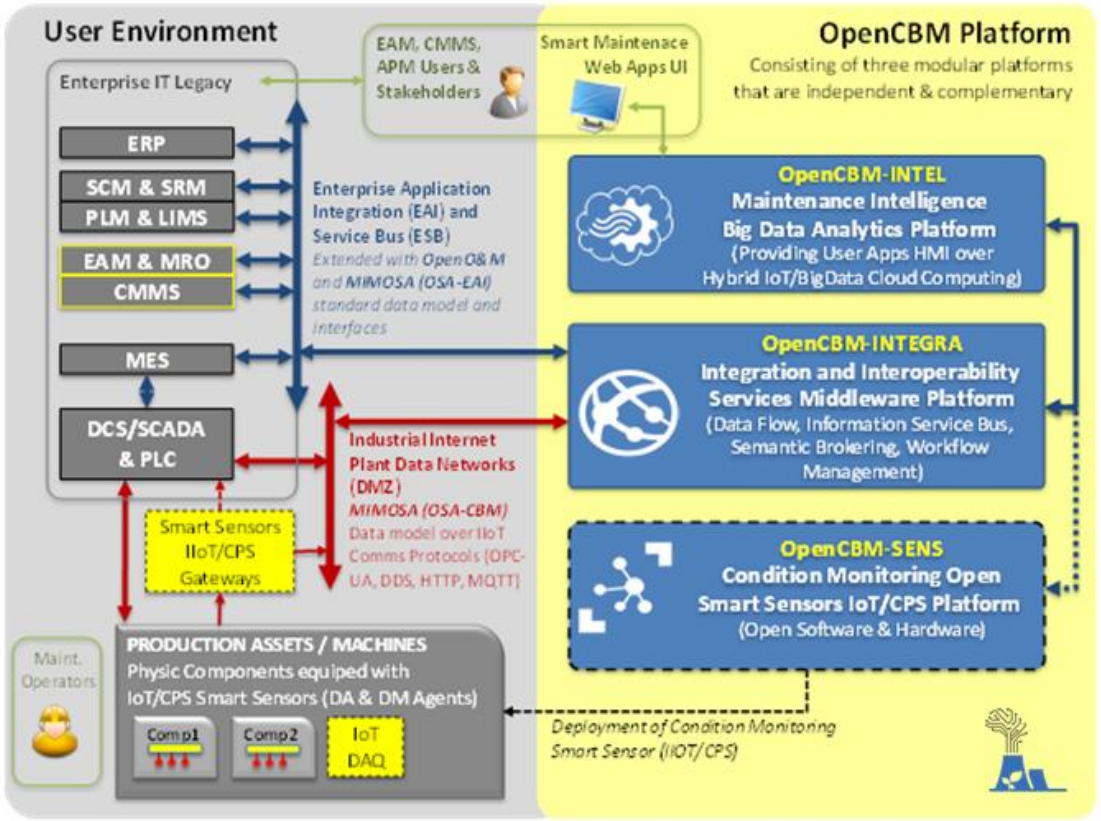
Smart Encoder:

- Industrial processes
- Machinery
- Productive environments
- High levels of precision

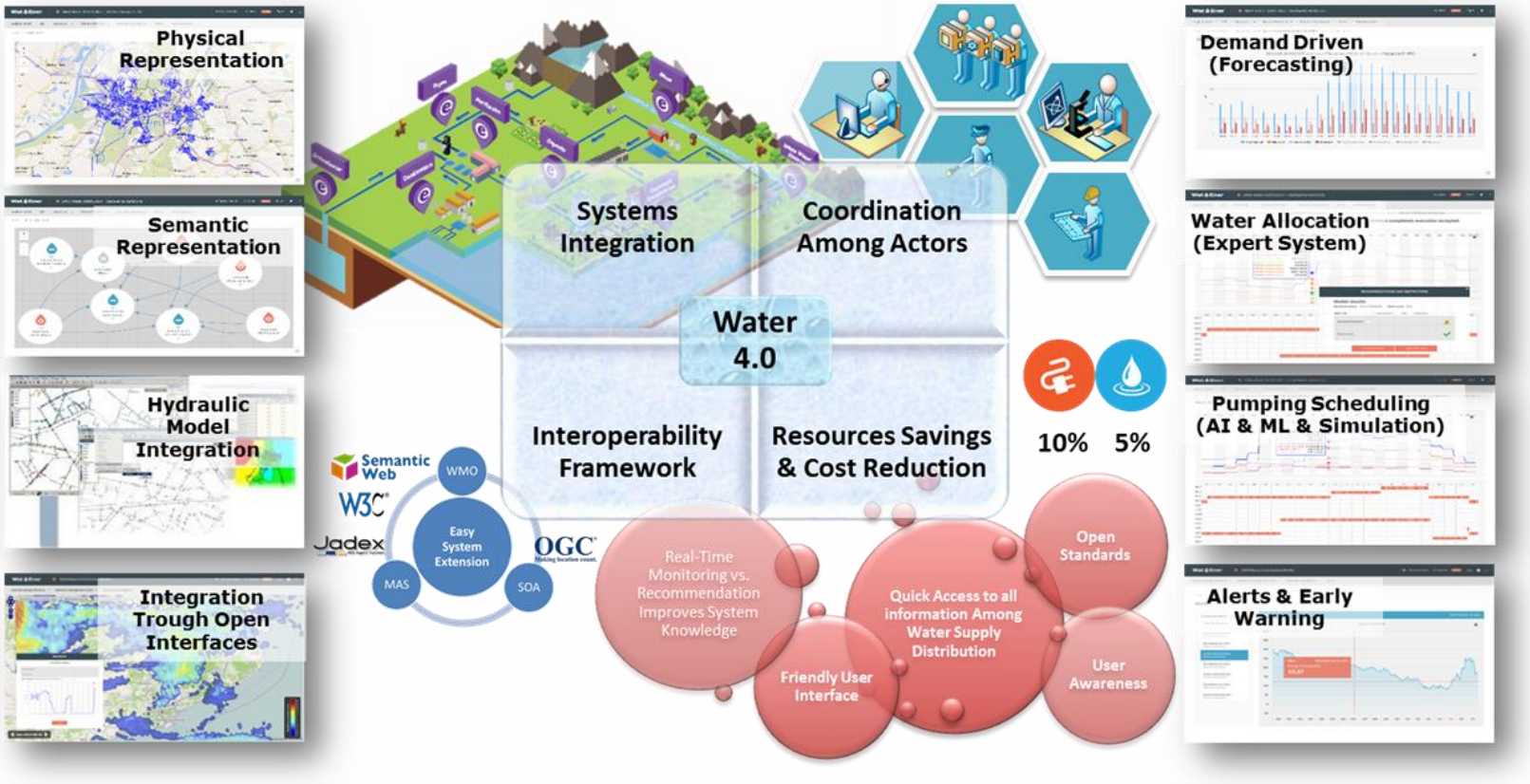
Analítica de dades



Analítica de dades en planta



...i entre plantes



Ciberseguretat Industrial

La Industria 4.0

La Industria 4.0

El risc a la Industria 4.0

L'equació del risc

Risc = Amenaça x Vulnerabilitat x Impacte

- Amenaça: Circumstancia o esdeveniment que te el potencial de causar danys.
- Vulnerabilitat: Debilitat que pot ser explotada per un adversari o a través d'un incident.
- Impacte: Quantitat de pèrdua o dany que es pot esperar després d'un atac exitós.

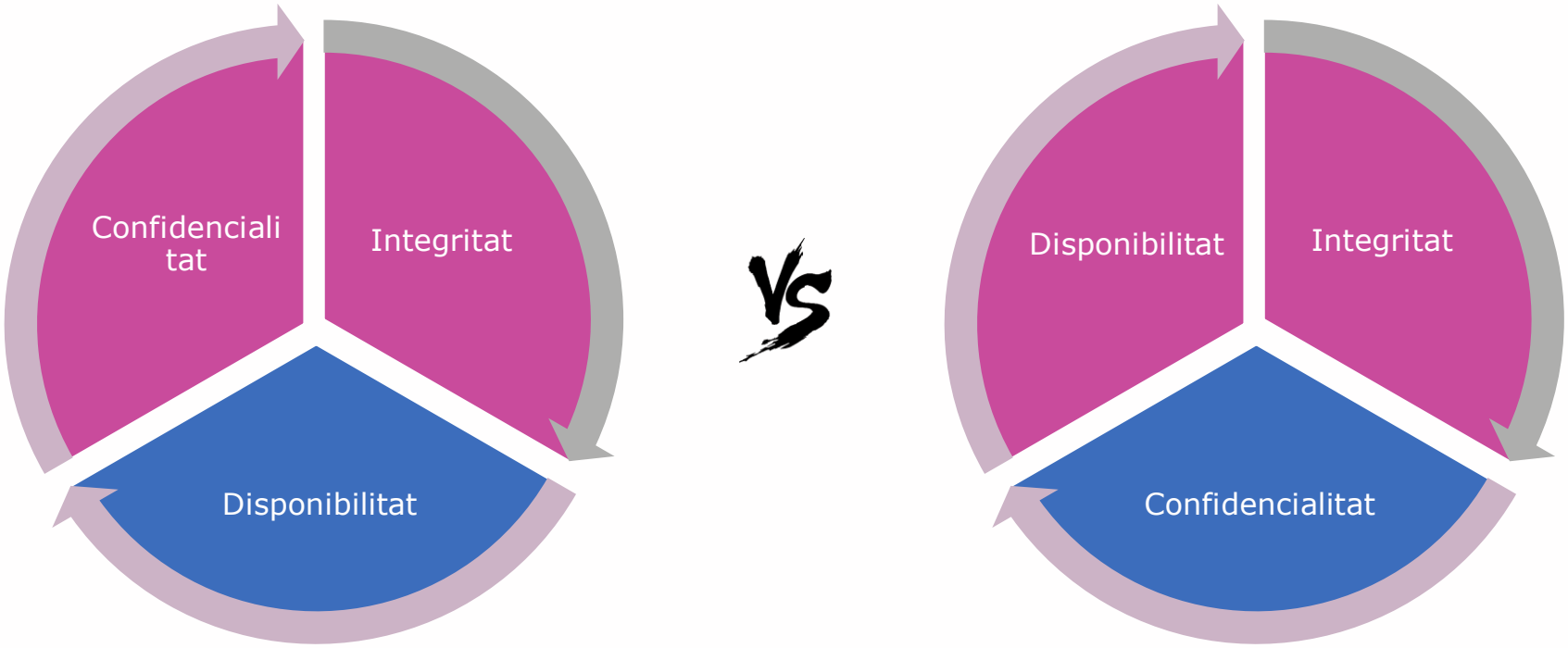
La realitat es...

- Les **vulnerabilitats** dels PLC son un fet.
- Xarxes sense fils? Es possible realitzar una **Denegació del Servei (DoS)** a qualsevol xarxa inalàmbrica amb una mínima inversió.
- Existeix un Firewall extern?, **què hi ha de la seguretat interna?**: la major part dels incidents són provocats des de dins (fallades tècniques, negligències, sabotatges, etc.).
- 80-90% dels SCADA estan connectats a la xarxa corporativa (molta vegades sense que el departament de TI/TO sigui conscient d'això): **sistemes a l'ombra** (shadow IT/OT).
- Els Sistema de Control i Automatització Industrial operen en un **entorn complex** (milers de senyals, múltiples xarxes, etc.).
- Les organitzacions **comparteixen** cada vegada més informació entre els seus sistemes d'informació corporatius i els seus sistemes de control de processos.

La realitat es...

- La **revelació de secrets** comercials/industrials o la **interrupció** en el flux d'informació no són les úniques conseqüències d'una fallada de seguretat.
- Les pèrdues de vides humanes, el dany mediambiental, la interrupció de la producció, l'incompliment reglamentari i el **compromís de la seguretat** en les operacions són conseqüències molt més greus.
- Aquestes conseqüències poden tenir ramificacions més enllà de la pròpia organització, ja que poden danyar greument la infraestructura de la regió o de la nació: **interdependències**.
- Les **amenaces** externes no són l'única preocupació, un acte involuntari i innocent pot suposar un greu **risc** de seguretat.

La realitat es...

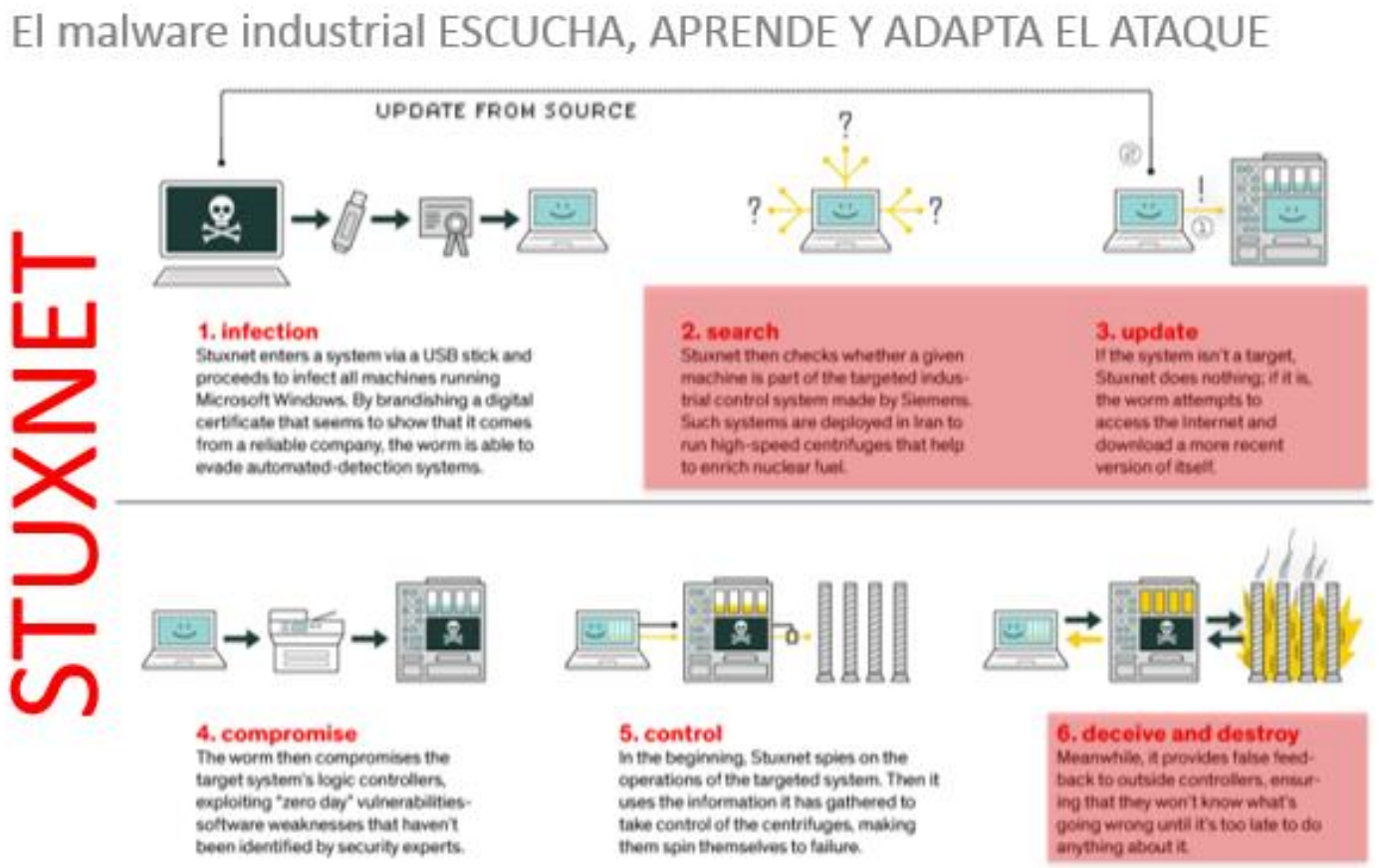


Àrea Industrial

- Habitualment:
  - No requereixen autenticació,
  - No requereixen, ni ofereixen, autorització,
  - No utilitzen xifrat,
  - No gestionen adequadament errors o excepcions.

- Per tant, habiliten diverses fonts de potencials debilitats:
  - Intercepció de dades,
  - Manipulació de dades,
  - Denegació de Servei (DoS),
  - Falsejament d'adreces (Address Spoofing),
  - Respostes no sol·licitades,
  - Segrest de sessions (Session Hijacking),
  - Manipulació de paquets/protocols,
  - Modificació de dades de registre (logs),
  - Accés no autoritzat.

Incidents


El malware industrial ESCUCHA, APRENDE Y ADAPTA EL ATAQUE
STUXNET
UPDATE FROM SOURCE
1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.
2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.
4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.
5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.
6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

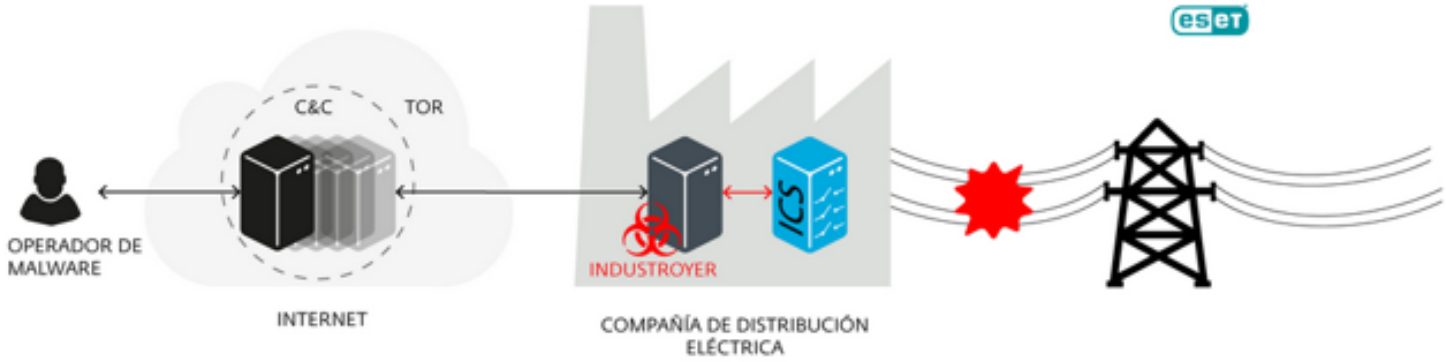
Incidents

El malware industrial ESCUCHA, APRENDE Y ADAPTA EL ATAQUE

Industroyer: la mayor amenaza para sistemas de control industrial desde Stuxnet

POR ANTON CHEREPANOV PUBLICADO 12 JUN 2017 - 09:16AM

AMENAZAS INFORMÁTICAS



INDUSTROYER

Incidents

ciberespionatge

En 2007, dos hackers accedieron a los **sistemas de control de semáforos** del departamento de tráfico de Los Angeles (California, EEUU).

- Apagaron los semáforos de cuatro intersecciones de la ciudad.
- Modificaron la configuración de los sistemas para impedir el acceso de los administradores legítimos.

En 2006 una **planta de tratamiento de aguas** (Pennsylvania, EEUU) sufrió una brecha de seguridad.

- Un ordenador portátil infectado permitió que *hackers* accedieran a los sistemas que controlaban la concentración de cloro en el agua potable.
- Afortunadamente sólo los utilizaron para enviar *spam*.

En 2005 la **presa Taum Sauk** (Missouri, EEUU) sufrió una brecha por la que salieron 4 millones de m^3 de agua en 12 minutos.

Ciberdelicte

- El causante fue un mal funcionamiento del *software* de control de las bombas de llenado.
- La presa siguió llenándose hasta sobrepasar su capacidad.

En enero de 2012 un hacker publicó una lista de IPs pertenecientes a **sistemas SCADA de organizaciones Israelíes**.

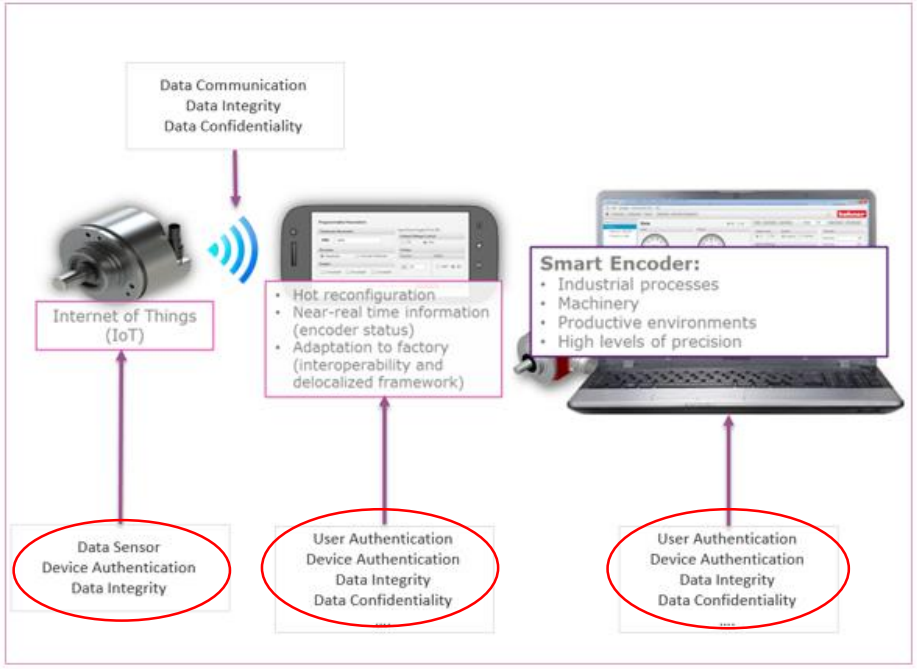
Además informó de que podían ser accedidos utilizando determinada contraseña.

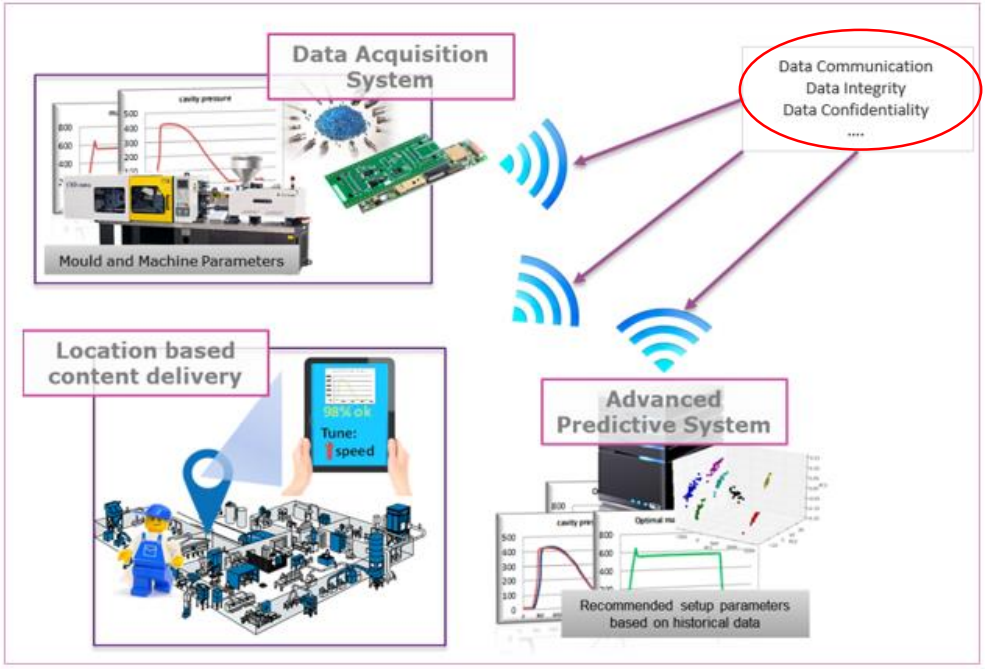
- La contraseña era: 100.
- Es la contraseña por defecto de los sistemas Simatic de Siemens.

Ciberterrorisme

On actuar

Ciberseguretat de tot el procés



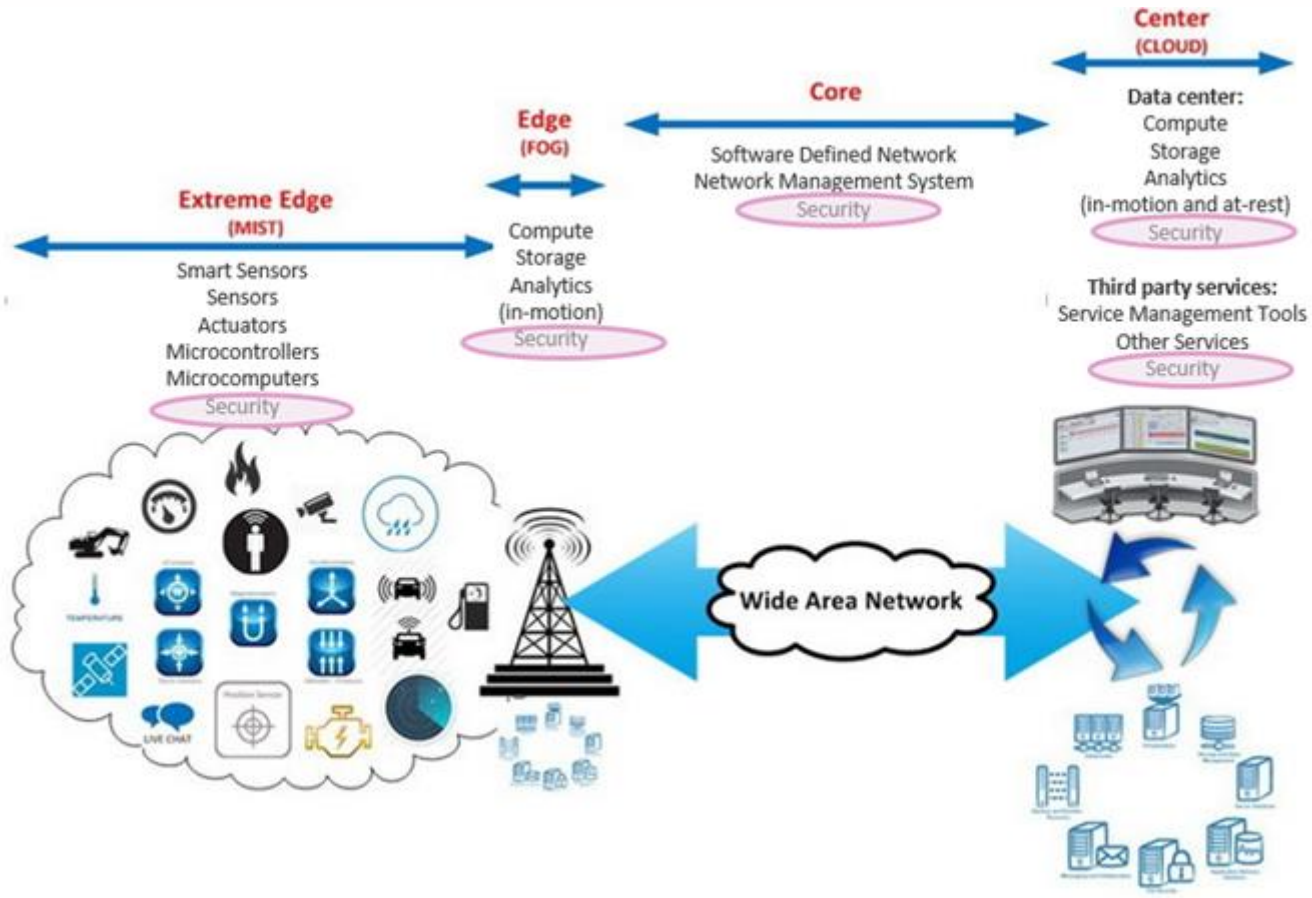


Dispositivo inteligente

Adquisición y analítica de datos en planta

Un ataque eficiente puede alterar o parar la producción de la planta por tiempo indefinido

Ciberseguretat a la Industria 4.0



Errors comuns

Errors de seguretat

- Creure que la xarxa es segura nomes perquè:
  - Està segmentada en diferents nivells,
  - Existeix un Firewall,
  - Els sistemes interns suposadament no estan connectats directament a Internet.

Propagació

- Regles massa permissives en els Firewalls:
  - Escàs filtratge de sortida.
  - Poques restriccions en els filtres.
- Sistemes mal administrats:
  - Serveis innecessaris.
  - Softwares no actualitzats.

Infecció

- No existeix una política d'us acceptable de USBs, Smartphones, portàtils, etc.
- Antivirus no actualitzats.
- Sistemes no parchejats.
- No es filtren els continguts web.
- No existeix un IDS.

Solucions

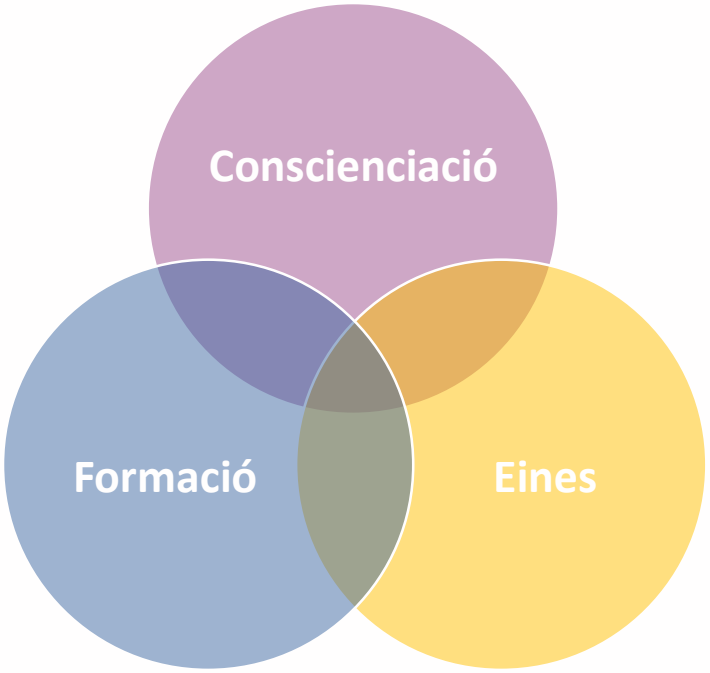
- Bona gestió:
  - Mantenir i actualitzar les polítiques de filtratge.
  - Revisar les consoles d'alarmes.
- Realitzar tests d'intrusió periòdicament.
- Securitzar els equips.
- Formació i conscienciació.

Ciberseguretat: com abordar el problema?

Es tracta d'un procés continu en el temps.

Security-by-Design: La ciberseguretat s'ha de tenir en compte des del primer minut de disseny i/o fabricació. Les mesures introduïdes des del principi milloren considerablement la resiliència dels dispositius i sistemes.

Formació i Conscienciació: Un dels aspectes essencials en el nou model d'Indústria 4.0 és ser conscients que els riscos als quals s'exposa una planta es veuen incrementats d'una manera considerable.



eurecat
Centre Tecnològic de Catalunya

GRÀCIES

info@eurecat.org
www.eurecat.org


www.twitter.com/eurecat_news


www.facebook.com/Eurecatorg